

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-285089

(43)Date of publication of application : 13.10.2005

(51)Int.Cl. G06F 12/14
H04L 9/32

(21)Application number : 2004-358517

(71)Applicant : NEC CORP
NIPPON HOSO KYOKAI <NHK>

(22)Date of filing : 10.12.2004

(72)Inventor : GOTO ATSUSHI
NISHIMOTO TOMONARI
BABA AKITSUGU
NAKAMURA HARUYUKI
ISHIKAWA KIYOHICO
KURIOKA TATSUYA

(30)Priority

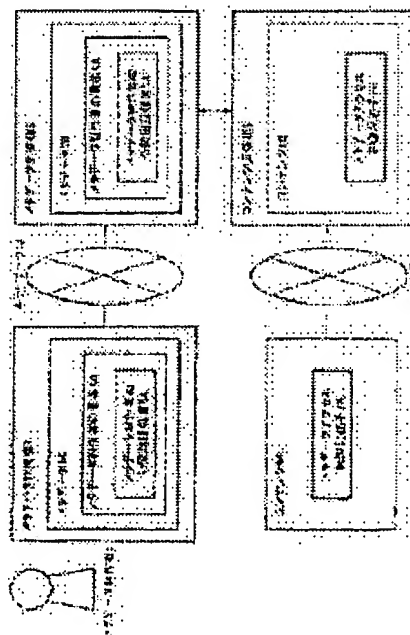
Priority number : 2004060085 Priority date : 04.03.2004 Priority country : JP

(54) ACCESS CONTROL METHOD, ACCESS CONTROL SYSTEM, META DATA CONTROLLER,
AND TRANSMISSION SYSTEM DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To control an enabled/disabled state of an access from meta data to contents.

SOLUTION: The access control method includes: a step for generating meta data 3A for a content 6A and embedding a digital signature 4A of a creator who has created the meta data as creator information in the created meta data 3A; a step for embedding an identifier 5A indicating from which meta data an access to the contents is allowed, in the license information required for reproducing the contents 6A; and an access enabled/disabled control step for controlling an access enabled/disabled state to the contents 6A from the created meta data 3A by comparing the digital signature 4A with the identifier 5A.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-285089

(P2005-285089A)

(43) 公開日 平成17年10月13日(2005.10.13)

(51) Int. Cl. ⁷G06F 12/14
H04L 9/32

F I

G06F 12/14 520C
G06F 12/14 540B
H04L 9/00 675B

テーマコード (参考)

5B017
5J104

審査請求 有 請求項の数 32 O L (全 22 頁)

(21) 出願番号 特願2004-358517 (P2004-358517)
 (22) 出願日 平成16年12月10日 (2004.12.10)
 (31) 優先権主張番号 特願2004-60085 (P2004-60085)
 (32) 優先日 平成16年3月4日 (2004.3.4)
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000004237
 日本電気株式会社
 東京都港区芝五丁目7番1号
 (71) 出願人 000004352
 日本放送協会
 東京都渋谷区神南2丁目2番1号
 (74) 代理人 100077838
 弁理士 池田 憲保
 (72) 発明者 後藤 淳
 東京都港区芝五丁目7番1号 日本電気株
 式会社内
 (72) 発明者 西本 友成
 東京都世田谷区砧一丁目10番11号 日
 本放送協会放送技術研究所内

最終頁に続く

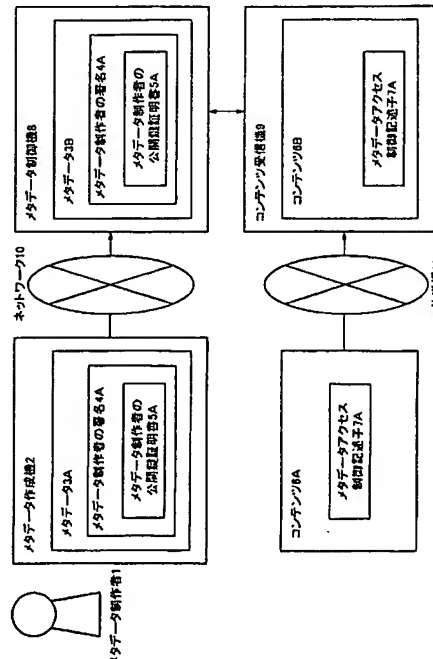
(54) 【発明の名称】 アクセス制御方法、アクセス制御システム、メタデータ制御機、及び送信系装置

(57) 【要約】

【課題】メタデータからコンテンツへのアクセスの可・不可を制御するアクセス制御方法の提供。

【解決手段】コンテンツ6Aに対するメタデータ3Aを制作し、制作されたメタデータ3A中に該メタデータを制作した制作者の電子署名4Aを制作者情報として埋め込むステップと、コンテンツ6Aを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子5Aを予め埋め込んでおくステップと、電子署名4Aと識別子5Aとを突き合わせることで、前記制作されたメタデータ3Aからコンテンツ6Aに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込みステップと、

前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおくステップと、

前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法。

【請求項 2】

請求項 1 に記載のアクセス制御方法において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御方法。

【請求項 3】

請求項 1 に記載のアクセス制御方法において、

前記制作者情報埋め込みステップは、コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す電子署名を、前記制作者情報として、埋め込む電子署名埋め込みステップであり、

前記アクセス可否制御ステップは、前記電子署名と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するステップであることを特徴とするアクセス制御方法。

【請求項 4】

請求項 3 に記載のアクセス制御方法において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御方法。

【請求項 5】

請求項 3 に記載のアクセス制御方法において、

前記電子署名は、公開鍵基盤（PKI）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするアクセス制御方法。

【請求項 6】

請求項 3 に記載のアクセス制御方法において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記アクセス可否制御ステップは、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするアクセス制御方法。

【請求項 7】

請求項 1 に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項 8】

請求項 1 に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項 9】

請求項 3 に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項 10】

請求項 3 に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項 11】

コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込み手段と、 10

前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおく識別子埋め込み手段と、

前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御手段とを有することを特徴とするアクセス制御システム。

【請求項 12】

請求項 11 に記載のアクセス制御システムにおいて、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御システム。 20

【請求項 13】

請求項 11 に記載のアクセス制御システムにおいて、

前記制作者情報埋め込み手段は、コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す電子署名を、前記制作者情報として、埋め込む電子署名埋め込み手段であり、

前記アクセス可否制御手段は、前記電子署名と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御する手段であることを特徴とするアクセス制御システム。

【請求項 14】

請求項 13 に記載のアクセス制御システムにおいて、 30

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御システム。

【請求項 15】

請求項 13 に記載のアクセス制御システムにおいて、

前記電子署名は、公開鍵基盤（PKI）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするアクセス制御システム。

【請求項 16】

請求項 13 に記載のアクセス制御システムにおいて、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、 40

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記アクセス可否制御ステップは、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするアクセス制御システム。

【請求項 17】

請求項 11 に記載のアクセス制御システムにおいて、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。 50

【請求項 18】

請求項 11 に記載のアクセス制御システムにおいて、

前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。

【請求項 19】

請求項 13 に記載のアクセス制御システムにおいて、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。

10

【請求項 20】

請求項 13 に記載のアクセス制御システムにおいて、

前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。

【請求項 21】

コンテンツを受信し再生する機能を有すると共に、前記コンテンツを再生するのに必要なライセンス情報に埋め込まれた、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を受信する機能を有するコンテンツ受信部に組合されて使用されるメタデータ制御機において、

20

前記コンテンツに対して制作されたメタデータと、制作されたメタデータ中に埋め込まれた、該メタデータを制作した制作者を示す制作者情報とを受信する機能と、

前記コンテンツ受信部から前記識別子を取得し、前記メタデータ中の前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツに対するアクセスの可否を制御するアクセス可否制御機能とを有することを特徴とするメタデータ制御機。

【請求項 22】

請求項 21 に記載のメタデータ制御機において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするメタデータ制御機。

30

【請求項 23】

請求項 21 に記載のメタデータ制御機において、

前記制作者情報が、前記メタデータを制作した制作者を示す電子署名であることを特徴とするメタデータ制御機。

【請求項 24】

請求項 23 に記載のメタデータ制御機において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするメタデータ制御機。

【請求項 25】

請求項 23 に記載のメタデータ制御機において、

前記電子署名は、公開鍵基盤（PKI）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするメタデータ制御機。

40

【請求項 26】

請求項 23 に記載のメタデータ制御機において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記メタデータ制御機は、前記公開鍵証明書情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツへのアクセスを許可し、前記制作されたメタデータ

50

に基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするメタデータ制御機。

【請求項 27】

コンテンツを受信系装置に送信するコンテンツ送信装置と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置とを有する送信系装置において、

前記メタデータ送信装置は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

前記コンテンツ送信装置は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

前記送信系装置は、前記受信系装置に、前記メタデータ送信装置から受信した前記制作者情報と前記コンテンツ送信装置から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたことを特徴とする送信系装置。

【請求項 28】

請求項 27 に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とする送信系装置。

【請求項 29】

請求項 27 に記載の送信系装置において、

前記制作者情報が、前記メタデータを制作した制作者を示す電子署名であることを特徴とする送信系装置。

【請求項 30】

請求項 29 に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とする送信系装置。

【請求項 31】

請求項 29 に記載の送信系装置において、

前記電子署名は、公開鍵基盤（PKI）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とする送信系装置。

【請求項 32】

請求項 29 に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記送信系装置は、前記受信系装置において、前記公開鍵証明書情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記受信系装置における、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記受信系装置に、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能とさせたことを特徴とする送信系装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタル放送におけるメタデータからコンテンツへのアクセス制御方法に関するものである。

【背景技術】

【0002】

サーバー型放送は、受信機に番組蓄積装置と通信接続機能を備えることで、放送時間に

10

20

30

40

50

拘束されない番組視聴を実現する。さらに、コンテンツプロバイダーがメタデータと呼ばれる番組関連情報を提供することで、ハイライト的な番組視聴などの多様な放送サービスを実現する。例えば、野球中継番組においてある打者の打撃シーンのみをダイジェストとして視聴するなどのサービスが挙げられる。このサービスは、コンテンツプロバイダーが、当該野球中継番組を示す番組名と前記打者のすべての打撃シーンの開始時間位置を示す情報とを含むメタデータを制作し、当該メタデータを視聴者に提供することにより、実現される。また、魅力あるメタデータを安価に制作するために、コンテンツプロバイダーだけでなく、ネットワークプロバイダーや、第三者機関やユーザなどがメタデータを制作することが想定されている。

【0003】

一方で、このメタデータを改竄したり、不正なメタデータを制作することで、CMのみを除いた番組視聴や、複数の番組のシーンをつないで別の番組を作成するなど、コンテンツプロバイダーの意向にもとづかない番組利用が行われる恐れがある。そのため、不正なメタデータの氾濫を防止するために、メタデータの改竄を防止し、番組ごとに、利用を許可するメタデータをコンテンツプロバイダーが指定できる必要がある。

【0004】

非特許文献1には、標準規格ARIB(Association of Radio Industries and Businesses) STD-B38(サーバー型放送における符号化、伝送及び蓄積制御方式)の概要が記載され、特に、サーバー型放送の概念が図示されている。

【0005】

ARIB STD-B38の規格中には、XML(Extensible Markup Language)形式による番組のメタデータの記述方法が定義されている。ARIB STD-B38の規格では、コンテンツに対する付加情報をメタデータに記述し再生端末に表示するだけでなく、メタデータの記述に基づいたコンテンツの部分再生などの再生制御のための情報を記述できるよう定義されている。メタデータからコンテンツを再生する機能を有する再生機を利用すると、コンテンツの部分再生やコンテンツ自体を編集せずにコンテンツのダイジェスト版を定義・再生することが可能となる。

【0006】

ここで、メタデータ自体はXMLで記述されるため、誰でも簡単に作成できる。そのため、コンテンツ自体にアクセスできれば誰でも簡単にコンテンツのダイジェスト版が作成できてしまうので、作成者Aが作成したメタデータからはアクセスを受け付けるが、Bが作成したメタデータからはアクセスを受け付けない、というようなコンテンツに対するアクセス制御を実現する必要があった。

【0007】

【非特許文献1】標準規格概要(放送分野) 規格番号: ARIB STD-B38 標準規格名: サーバー型放送における符号化、伝送及び蓄積制御方式、[online]、社団法人電波産業会、[2004年1月29日検索]、インターネット<URL: http://www.arib.or.jp/tyosakenkyu/kikaku_hoso/hoso_std-b038.html>

【発明の開示】

【発明が解決しようとする課題】

【0008】

本発明の目的は、メタデータとコンテンツが配信され、メタデータによってコンテンツの再生制御の機能が実現されるサーバー型放送において、メタデータの制作者によってコンテンツへのアクセスの可・不可を制御するアクセス制御方法を提供することにある。

【0009】

本発明の別の目的は、上述のアクセス制御方法を実施するアクセス制御システムを提供することにある。

【0010】

本発明の他の目的は、メタデータの制作者によってコンテンツへのアクセスの可否を制御するメタデータ制御機を提供することにある。

10

20

30

40

50

【0011】

本発明の更に他の目的は、受信系装置に、メタデータの制作者によってコンテンツへのアクセスの可否を制御可能とさせる送信系装置を提供することにある。

【課題を解決するための手段】

【0012】

本発明によれば、

コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込みステップと、

前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおくステップと、

前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法が得られる。

10

【0013】

更に、本発明によれば、

コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込み手段と、

前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおく識別子埋め込み手段と、

前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御手段とを有することを特徴とするアクセス制御システムが得られる。

20

【0014】

また、本発明によれば、

コンテンツを受信し再生する機能を有すると共に、前記コンテンツを再生するのに必要なライセンス情報に埋め込まれた、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を受信する機能を有するコンテンツ受信部に組合されて使用されるメタデータ制御機において、

前記コンテンツに対して制作されたメタデータと、制作されたメタデータ中に埋め込まれた、該メタデータを制作した制作者を示す制作者情報とを受信する機能と、

30

前記コンテンツ受信部から前記識別子を取得し、前記メタデータ中の前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツに対するアクセスの可否を制御するアクセス可否制御機能とを有することを特徴とするメタデータ制御機が得られる。

【0015】

更に、本発明によれば、

コンテンツを受信系装置に送信するコンテンツ送信装置と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置とを有する送信系装置において、

前記メタデータ送信装置は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

40

前記コンテンツ送信装置は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

前記送信系装置は、前記受信系装置に、前記メタデータ送信装置から受信した前記制作者情報と前記コンテンツ送信装置から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたことを特徴とする送信系装置が得られる。

【発明の効果】

50

【0016】

本発明によれば、メタデータの制作者を示す制作者情報（署名値）とコンテンツを再生するのに必要なライセンス情報に埋め込まれた識別子（メタデータアクセス制御記述子）を突き合わせることで、メタデータからコンテンツへのアクセス可否を判断することが出来る。

【発明を実施するための最良の形態】

【0017】

以下に述べる本発明の実施例では、メタデータ中に埋め込まれる、該メタデータを制作した制作者を示す制作者情報が、その制作者の電子署名である場合を例に説明するが、制作者情報は、電子署名に限らず、メタデータを制作した制作者を示すその他の情報であっても良い。ここで、メタデータを制作した制作者とは、メタデータの中にメタデータのインスタンス（実体）自体を作成した作成者か、或いは、そのメタデータを追加編集した制作者かである。

【0018】

具体的には、以下の実施例では、ARIB STD-B38で定義されたメタデータの中にメタデータのインスタンス（実体）自体を作成した作成者（或いはそのメタデータを追加編集した制作者）の電子署名（XML署名）を制作者情報として埋め込み、メタデータの作成者（或いは追加編集した制作者）を同定する。一方、コンテンツには、どのメタデータからのアクセスを許可するかを判断するための識別子を埋め込み、電子署名（XML署名）と識別子とを両者を突き合わせることで、制作されたメタデータからコンテンツに対するアクセスの可否を制御する。

【0019】

以下、本発明の実施例について図面を参照して説明する。

【0020】

図1を参照すると、本発明の第1の実施例によるアクセス制御システムが示されている。このアクセス制御システムは、メタデータからコンテンツへのアクセスを制御するためのものである。

【0021】

このアクセス制御システムは、既に作成されたコンテンツ6Aに対するメタデータ3Aを作成するのに使用されるメタデータ作成機2を有する。すなわち、メタデータ作成機2を保持しているメタデータ制作者1が、既に作成されたコンテンツ6Aに対するメタデータ3Aをメタデータ作成機2上で作成する。

【0022】

ここで、コンテンツ6Aには、どのメタデータからコンテンツ6Aへのアクセスを許可するかを示すメタデータアクセス制御記述子7Aが埋め込まれている。典型的には、メタデータアクセス制御記述子7Aは、コンテンツ6Aへのアクセスが許可されるメタデータの制作者を示している。これは本発明の特徴の一つである。

【0023】

図2を参照すると、メタデータ制作者1によって作成されたメタデータ（署名前メタデータ）が示されている。署名前メタデータにおいて、制作者の作成部13の一つには、例えば、前述の野球中継番組のある打者のすべての打撃シーンの開始時間位置を示す情報が、メタデータのインスタンスとして、入れられる。

【0024】

図1に戻って、メタデータ制作者1は、自身を証明する公開鍵証明書とそれに対応する秘密鍵を有している。メタデータ制作者1は、メタデータ3Aの作成が終了すると、メタデータ作成機2上で、メタデータ3AにXML-Signatureで定義されるXML署名4Aと署名に利用した公開鍵証明書5Aを付加することで、作成者署名付きのメタデータを作成する。

【0025】

図3を参照すると、上述の作成者署名付きのメタデータ3Aが示されている。署名者の公開鍵証明書5Aは、バイナリをBase64でエンコードした形でXML形式の制作者1の署

名 4 A に埋め込まれる。

【 0 0 2 6 】

図 1 に戻って、コンテンツ 6 A は、放送用の通信手段である放送網 1 1 を使って利用者に配布され、メタデータ 3 A は、ネットワーク（インターネット等の通信ネットワーク）1 0 を使って利用者に配布される。利用者は、ネットワーク 1 0 に接続され、メタデータ作成機 2 から配布されたメタデータ 3 A をメタデータ 3 B として取得するメタデータ制御機 8 と、放送網 1 1 からのコンテンツ 6 A をコンテンツ 6 B として取得するコンテンツ受信機 9 とを保持する。コンテンツ受信機 9 は、コンテンツ再生機能をも有するものである。利用者は、メタデータ制御機 8 を利用して、配送されてきたメタデータ 3 B（3 A と同じ）にアクセスし、メタデータ 3 B からコンテンツ 6 B（6 A と同じ）へのアクセスが可能
10

【 0 0 2 7 】

上述では、コンテンツ 6 A を放送網 1 1、メタデータ 3 A をネットワーク 1 0 を使って利用者に配布する方法を示したが、コンテンツ 6 A をネットワーク、メタデータ 3 A を放送網で配布してもよい。また、コンテンツ 6 A 及びメタデータ 3 A を両方とも放送網で配布してもよいし、コンテンツ 6 A 及びメタデータ 3 A を両方ともネットワークで配布してもよい。

【 0 0 2 8 】

この際、メタデータ制御機 8 が、メタデータ 3 B からコンテンツ 6 B にアクセスするとき
20

きは、まず、メタデータ 6 B に付与されているメタデータ制作者の署名 4 A を検証しメタデータ 3 B が改竄されていないことを確認する。次に、メタデータ制作者の公開鍵証明書 5 A の中に記述されている公開鍵証明書の所有者の情報が格納されているサブジェクト(subject)領域の値を取得し、メタデータ 3 A の作成者を同定する。続いて、メタデータ制御機 8 は、コンテンツ受信機 9 にアクセスし、コンテンツ 6 B のメタデータアクセス制御記述子 7 A を取得する。メタデータ制御機 8 は、メタデータアクセス制御記述子 7 A と公開鍵証明書の所有者の情報（RFC3280 で規定される公開鍵証明書の subject）を突き合わせることで、メタデータからコンテンツへのアクセス可能かどうか判断する。

【 0 0 2 9 】

すなわち、メタデータ制御機 8 は、公開鍵証明書の所有者の情報（RFC3280 で規定される公開鍵証明書の subject）がメタデータアクセス制御記述子 7 A にアクセスを許可するメタデータの制作者として記述されている場合には、メタデータ 3 B からコンテンツ 6 B へのアクセスを許可され、メタデータ 3 B に基づいたコンテンツ 6 B のダイジェスト映像など
30

【 0 0 3 0 】

ここで、メタデータアクセス制御記述子 7 A に、あらゆるメタデータ制作者をアクセス許可するものとして記述しておいた場合には、どのメタデータ制作者でも、自分が作ったメタデータに基づいたコンテンツ 6 B のダイジェスト映像などを自由に見ることが出来る
。

【 0 0 3 1 】

また、メタデータ制御機 8 は、公開鍵証明書の所有者の情報（RFC3280 で規定される公開鍵証明書の subject）がメタデータアクセス制御記述子 7 A に記述されているメタデータの制作者として識別（或いは、特定）される場合でも、メタデータ 3 B からコンテンツ 6 B へのアクセスを許可され、メタデータ 3 B に基づいたコンテンツ 6 B のダイジェスト映像など
40

【 0 0 3 2 】

なお、前記電子署名は、公開鍵基盤（PKI）技術にもとづき前記制作者としての署名者を特定することができるものであれば良い。

【 0 0 3 3 】

図 4 を参照すると、本発明の第 2 の実施例によるアクセス制御システムが示されている
50

。このアクセス制御システムは、上述したコンテンツ 6 A (図 1) を作成するコンテンツ作成機 2 2 と、メタデータ作成機 2 (図 1) 及びコンテンツ作成機 2 2 とメタデータ制御機 8 (図 1) 及びコンテンツ受信機 9 (図 1) との間に接続されたメタデータ制御機 2 9 及びコンテンツ受信及び送信機 3 0 とを、更に有する。図示の例では、メタデータ制御機 2 9 及びコンテンツ受信及び送信機 3 0 は、メタデータ作成機 2 及びコンテンツ作成機 2 2 にネットワーク 2 5 を介して接続されると共に、メタデータ制御機 8 及びコンテンツ受信機 9 にネットワーク 1 0 及び放送網 1 1 を介して接続される。

【 0 0 3 4 】

この場合、ネットワーク 2 5 は、ネットワーク 1 0 と同じネットワークが用いられても良い。或いは、メタデータ作成機 2 及びコンテンツ作成機 2 2 とメタデータ制御機 2 9 及びコンテンツ受信及び送信機 3 0 との接続に、ネットワーク 2 5 を用いる代りに、ネットワーク 1 0 及び放送網 1 1 を用いても良い。

【 0 0 3 5 】

このアクセス制御システムにおいて、コンテンツ受信及び送信機 3 0 は、ネットワーク 2 5 からのコンテンツ 6 A をコンテンツ 6 A' として取得する図 1 のコンテンツ受信機 9 (コンテンツ再生機能をも有する) の機能と、コンテンツ 6 A' を放送網 1 1 を介して送信する送信機の機能とを有する。コンテンツ受信及び送信機 3 0 に続いて、コンテンツ受信機 9 は、放送網 1 1 からのコンテンツ 6 A' をコンテンツ 6 B として取得する。

【 0 0 3 6 】

メタデータ制御機 2 9 は、ネットワーク 2 5 からのメタデータ 3 A をメタデータ 3 A' として取得する。メタデータ制御機 2 9 は、ネットワーク 2 5 からのメタデータ 3 A をメタデータ 3 A' として取得する。メタデータ制御機 2 9 は、図 1 で述べたメタデータ制御機 8 と同様に、メタデータ制作者 1 がコンテンツ 6 A' 内のメタデータアクセス制御記述子 7 A にアクセスを許可するメタデータの制作者として記述されているか、識別 (或いは、特定) される場合には、メタデータ 3 A' からコンテンツ 6 A' へのアクセスを許可される。メタデータ制御機 2 9 及びコンテンツ受信及び送信機 3 0 の利用者 (メタデータ制作者 3 4) は、メタデータ 3 A' に基づいたコンテンツ 6 A' のダイジェスト映像などを見ることが出来る。

【 0 0 3 7 】

メタデータ制御機 2 9 は、メタデータ 3 A' をネットワーク 1 0 を介して送信する機能をも有する。メタデータ制御機 2 9 に続いて、メタデータ制御機 8 は、ネットワーク 1 0 からのメタデータ 3 A' をメタデータ 3 B として取得する。メタデータ制御機 8 及びコンテンツ受信機 9 の利用者也、図 1 で述べたとおり、メタデータ制作者 1 がコンテンツ 6 B 内のメタデータアクセス制御記述子 7 A にアクセスを許可するメタデータの制作者として記述されているか、識別 (或いは、特定) される場合には、メタデータ 3 B からコンテンツ 6 B へのアクセスを許可され、メタデータ 3 B に基づいたコンテンツ 6 B のダイジェスト映像などを見ることが出来る。

【 0 0 3 8 】

このアクセス制御システムにおいて、メタデータ作成機 2 でメタデータ制作者 1 がコンテンツ 6 A に対するメタデータ 3 A を作成し、メタデータ制御機 2 9 でメタデータ制作者 3 4 がメタデータ 3 A に追加編集を加えて、メタデータ 3 A' としたとする。

【 0 0 3 9 】

図 5 を参照すると、メタデータ制御機 2 9 でメタデータ制作者 3 4 がメタデータ 3 A に追加編集を加えた場合の署名された XML 形式のメタデータ 3 A' が示されている。この場合、署名された XML 形式のメタデータ 3 A' 内には、メタデータ制作者 1 とメタデータ制作者 3 4 の二人が作成したメタデータがメタデータ制作者 1 の作成部 1 3 (図 2) とメタデータ制作者 3 4 の作成部 3 7 とが混在し、メタデータ制作者 1 及びメタデータ制作者 3 4 の XML 署名がメタデータ制作者 1 の署名 4 A (図 2) 及びメタデータ制作者 3 4 の署名 3 9 としてメタデータ 3 A' に埋め込まれることになる。

【 0 0 4 0 】

10

20

30

40

50

図 4 において、しかしながら、署名 3 9 内の XML 署名の公開鍵証明書の所有者（メタデータ制作者 3 4）がコンテンツ 6 A' 内のメタデータアクセス制御記述子 7 A にアクセスを許可するメタデータの制作者として記述されていないか、識別（或いは、特定）されない場合には、メタデータ制御機 2 9 において、メタデータ 3 A' からコンテンツ 6 A' へのアクセスは許可されず、メタデータ 3 A' に基づいたコンテンツ 6 A' のダイジェスト映像などは見ることが出来ない。

【0041】

このように、メタデータ作成者 3 4 が、コンテンツ受信及び送信機 3 0 において受信したコンテンツ 6 A' にアクセスするメタデータを作成部 3 7 としてメタデータ制御機 2 9 において、追加したとしても、コンテンツ作成機 2 2 でメタデータアクセス制御記述子 7 A を作成する段階で権限を与えられていなければ、そのメタデータを有効に機能させない、メタデータからコンテンツへのアクセス制御が、実現する。

【0042】

ここで、図 4 において、受信系装置が、メタデータ制御機 2 9 とコンテンツ受信及び送信機 3 0 との組合せ、或いは、メタデータ制御機 8 とコンテンツ受信機 9 との組合せであるとする。更に、図 4 において、送信系装置が、コンテンツを前記受信系装置に送信するコンテンツ送信装置（コンテンツ作成機 2 2）と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置（メタデータ作成機 2）とを有するものとする。

【0043】

この場合、メタデータ送信装置（メタデータ作成機 2）は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者の電子署名を埋め込んだ状態にて前記受信系装置に送信する機能を有し、コンテンツ送信装置（コンテンツ作成機 2 2）は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有するものである。そして、前記送信系装置は、前記受信系装置に、前記メタデータ送信装置（メタデータ作成機 2）から受信した前記電子署名と前記コンテンツ送信装置（コンテンツ作成機 2 2）から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたものである。

【0044】

次に、図 4 の実施例の各部分について詳細に説明する。

【0045】

（メタデータ制作機 2）

図 6 を参照すると、メタデータ作成機 2 は、IC (Integrated Circuit) カードリーダライタ 4 5 が接続された、パーソナルコンピュータなどの情報処理装置である。メタデータ作成機 2 は、例えばソフトウェアで実現されるメタデータ作成部 4 1 とメタデータ送信部 4 2 とから構成される。メタデータ作成機 4 0 は、コンテンツ 6 A（図 4）に対応するメタデータ 3 A（図 4）を作成する機能、作成したメタデータ 3 A に対して電子署名を付与する機能を有し、電子署名に利用する公開鍵証明書、秘密鍵を格納した IC カード 4 6 へアクセスするための機能を有し、IC カードリーダライタ 4 5 が接続される。

【0046】

メタデータ作成部 4 1 は、コンテンツ 6 A に対応するメタデータ 3 A を作成する機能を有し、作成したコンテンツ 6 A に対し、電子署名を付加する機能として署名生成部 4 3 を有するソフトウェアで構成される。また、作成したメタデータ 3 A を使いコンテンツ 6 A を再生するためのコンテンツ再生制御部 4 4 を有する。

【0047】

メタデータ送信部 4 2 は、メタデータ作成部 4 1 で作成されたメタデータ 3 A をインターネット等の通信ネットワーク 2 5（図 4）を介してメタデータ制御機 2 9（図 4）へ転送する機能を有する。

10

20

30

40

50

【0048】

署名生成部43は、作成されたメタデータ3Aに対して電子署名を付与する機能を有する。署名対象文書に対し、W3Cの規格であるXML-Signature形式の署名文書を作成し、署名のためのハッシュ値を生成、ICカードリーダーライター45を介したICカード46により署名値を生成し、生成された署名値をXML署名文書に埋め込むことにより署名を実行する。また、ICカード46に格納されている署名者の公開鍵証明書を署名対象文書に埋め込む機能も有する。

【0049】

ICカード46は、秘密鍵と公開鍵証明書が格納でき、内部で暗号計算を実行できる機能を有する。ICカードリーダーライター45経由で、署名対象文書のハッシュ値が渡されると、それを暗号化することにより署名値を生成し、それをICカードリーダーライター45経由で署名生成部43へ返却する。

10

【0050】

ICカードリーダーライター45は、パーソナルコンピュータなどの情報処理装置からの命令によりICカード46内の情報を読み取る機能、およびICカード46にICカード46内に格納された鍵を用いた電子署名のための暗号計算の実行を命令する機能を有する。

【0051】

コンテンツ再生制御部44は、メタデータ3Aの内容に従いコンテンツ作成機22（図4）へコンテンツの部分再生を命令する機能を有する。

【0052】

（メタデータ制御機29（或いは8））

図7を、図4と併せ参照して、メタデータ制御機47は、ICカードリーダーライター52が接続されたパーソナルコンピュータなどの情報処理装置である。メタデータ制御機47は、ソフトウェアプログラムで実現される署名生成・検証機能部49とコンテンツ再生制御部50とを含むメタデータ編集部48と、メタデータ送受信部51とから構成される。

20

【0053】

ICカードリーダーライター52及びICカード53は、メタデータ作成機40に接続されているものと同等のものである。

【0054】

メタデータ編集部48は、メタデータ3A'（或いは3B）を編集する機能と、編集した部分に対し、署名生成・検証機能部49とICカードリーダーライター52とICカード53とを利用して、電子署名を付与する機能と、署名生成・検証機能部49を使って、メタデータ3A'（或いは3B）に付与された署名および証明書を検証する機能と、コンテンツ6A'（或いは6B）の再生制御を行うコンテンツ再生制御部50を有する。

30

【0055】

署名生成・検証機能部49は、メタデータ作成機2と同様の署名生成機能と、与えられたメタデータの署名値を検証する機能と、証明書の検証機能を有する。

【0056】

コンテンツ再生制御部50は、メタデータ3A'（或いは3B）の内容に従いコンテンツ受信及び送信機30（或いはコンテンツ受信機9）へコンテンツ6A'（或いは6B）の部分再生を命令する機能を有する。また、コンテンツ再生制御部50は、再生時にメタデータ3A'（或いは3B）からコンテンツ6A'（或いは6B）へアクセス可能かどうかを判断するために利用するメタデータアクセス制御記述子7Aを、コンテンツ6A'（或いは6B）から取得する機能を有する。また、コンテンツ再生制御部50は、メタデータ3A'（或いは3B）に埋め込まれているメタデータ作成書署名の中からメタデータ制作者の公開鍵証明書を取得し、公開鍵証明書の所有者から署名者を同定する機能を有する。同定した署名者と、取得したメタデータアクセス制御記述子7Aを比較しコンテンツ6A'（或いは6B）へのアクセス可否を判断する機能を有する。

40

【0057】

（コンテンツ作成機22内の送信機）

50

図 8 を、図 4 と併せ参照して、コンテンツ作成機 2 2 内の送信機は、コンテンツを記憶しているコンテンツ記憶部 5 4、符号化部 5 5、スクランブル部 5 6 をもつコンテンツ生成手段 5 7 と、コンテンツ鍵 Kc 生成のためのコンテンツ鍵生成部 5 9、メタデータアクセス制御情報生成部 6 0、コンテンツを再生するのに必要なライセンス情報 (Kc 伝送用 ECM (Entitlement Control Message)/EMM (Entitlement Management Control Message)) を生成する Kc 伝送用 ECM/EMM 生成部 6 1 をもつ鍵生成手段 5 8 と、コンテンツ生成手段 5 7 で生成した暗号化コンテンツと、鍵生成手段 5 8 で生成した鍵を多重化する多重化手段 6 3 から構成される。

【 0 0 5 8 】

コンテンツ記憶部 5 4 は、映像、音声またはデータをコンテンツ 6 A として記憶するハードディスクなどの記憶装置で構成される。 10

【 0 0 5 9 】

符号化部 5 5 は、映像、音声またはデータを MPEG (Motion Picture Experts Group)-2 TS (Transport Stream) に符号化する符号化装置で構成される。

【 0 0 6 0 】

コンテンツ鍵生成部 5 9 は、共通鍵暗号化方式でコンテンツを暗号化するための暗号鍵 (コンテンツ鍵 Kc) をコンテンツ毎に生成し、コンテンツを識別するためのコンテンツ識別を割り当て、コンテンツ識別ごとにコンテンツ鍵を管理する。

【 0 0 6 1 】

スクランブル部 5 6 は、符号化したコンテンツを、コンテンツ鍵生成部 5 9 で生成したコンテンツ鍵で暗号化し、暗号化コンテンツを生成する。 20

【 0 0 6 2 】

メタデータアクセス制御情報生成部 6 0 は、コンテンツ 6 A に対してメタデータ利用を許可するための、メタデータアクセス制御記述子 7 A を生成する。メタデータアクセス制御記述子 7 A は、メタデータ制作者自身の識別コードであるメタデータ制作者識別、メタデータ制作者の属性 (コンテンツプロバイダー兼メタデータ制作者、専業メタデータ制作者、利用者 (ユーザ) など) を示すメタデータ制作者種別から構成される。

【 0 0 6 3 】

Kc 伝送用 ECM/EMM 生成部 6 1 は、コンテンツ鍵 Kc、メタデータアクセス制御情報 (メタデータアクセス制御記述子 7 A)、およびワーク鍵或いはマスター鍵 6 2 を含んだ、ARIB 30 -STDB25「デジタル放送におけるアクセス制御方式」で規定されるセクション形式の Kc 伝送用 ECM または Kc 伝送用 EMM を生成する。すなわち、Kc 伝送用 ECM/EMM 生成部 6 1 において、メタデータアクセス制御情報 (メタデータアクセス制御記述子 7 A) がコンテンツを再生するために必要となるライセンス情報 Kc 伝送用 ECM または Kc 伝送用 EMM に埋め込まれる。Kc 伝送用 ECM は、ワーク鍵 6 2 で、Kc 伝送用 EMM はマスター鍵 6 2 で暗号化する。マスター鍵 6 2 は、受信機ごとに付与される共通鍵暗号化方式の暗号鍵である。ワーク鍵 6 2 は、事業者ごとなどの単位で付与される共通鍵暗号化方式の暗号鍵であり、Kc 伝送用 ECM を受信させたい受信機に対して予め共有化される暗号鍵であり、おのこの受信機をグループ化するための暗号鍵である。すなわち、Kc を予めワーク鍵を共有化した受信機に対して一斉配信したい場合は、Kc 伝送用 ECM を用い、各々の受信機に個別に Kc を配信したい場合は 40、Kc 伝送用 EMM を用いる。

【 0 0 6 4 】

Kc 伝送用 ECM/EMM (ライセンス情報) を放送により送る場合、多重化手段 6 3 の多重化部 6 4 は、コンテンツ生成手段 5 7 の暗号化コンテンツ、ワーク鍵で暗号化した Kc 伝送用 ECM/EMM の多重化を行い変調し放送として送出する。

【 0 0 6 5 】

ここで、各々の受信機に個別に Kc を配信する場合には Kc 伝送用 EMM (ライセンス情報) を TCP/IP (Transmission Control Protocol/Internet Protocol) を利用した通信ネットワークを用いて個別に配信する。

【 0 0 6 6 】

(コンテンツ受信及び送信機 30 内の送信機)

コンテンツ受信及び送信機 30 内の送信機も、図 8 に示したコンテンツ作成機 22 内の送信機と同様の構成を有する。ただし、コンテンツ生成手段 57 のコンテンツ記憶部 54 には、コンテンツ受信及び送信機 30 内の受信機にて受信したコンテンツ作成機 22 からのコンテンツ (映像、音声またはデータ) を記憶するものである。

【0067】

(コンテンツ受信機 9)

図 9 を、図 4 と併せ参照して、コンテンツ受信機 9 は、デスクランブル部 67、復号化部 69 をもつコンテンツ復号手段と、Kc 伝送用 ECM/EMM 復号部 70、コンテンツ鍵記憶部 72、メタデータアクセス制御情報記憶部 73 をもつセキュリティモジュール 74 と、暗号化コンテンツ 66 と鍵情報との分離を行う分離手段とから構成される。 10

【0068】

セキュリティモジュール 74 は、外部から不正に情報を取り出すことができない耐タンパーなモジュールであり、IC カード等で構成される。このセキュリティモジュール 74 は、第 3 者機関で厳重に発行、管理が行われる。

【0069】

分離部 65 は、受信した放送を復調し、MPEG-2 TS レベルで、暗号化コンテンツ 66 と、Kc 伝送用 ECM/EMM 76 を分離する。

【0070】

Kc 伝送用 ECM/EMM 復号化部 70 は、受信した Kc 伝送用 ECM をワーク鍵 71 で、Kc 伝送用 EMM をマスター鍵 71 で暗号復号し、コンテンツ鍵 (Kc) 68 及びメタデータアクセス制御情報 (メタデータアクセス制御記述子 7A) 75 を取り出しコンテンツ鍵記憶部 72 及びメタデータアクセス制御情報記憶部 73 に記憶する。このように、コンテンツ鍵 (Kc) 68 及びメタデータアクセス制御情報 (メタデータアクセス制御記述子 7A) 75 をセキュリティモジュール 74 で安全に記憶する。 20

【0071】

この際、コンテンツ鍵記憶部 72 は、コンテンツ識別ごとにコンテンツ鍵 68 を記憶する。

【0072】

メタデータアクセス制御情報記憶部 73 は、コンテンツ識別ごとにメタデータアクセス制御情報 (メタデータアクセス制御記述子 7A) 75 を記憶する。 30

【0073】

デスクランブル部 67 は、セキュリティモジュール 74 から得られるコンテンツ鍵 68 で、暗号化コンテンツを暗号復号する。

【0074】

復号化部 69 は、受信した MPEG-2 TS で符号化したコンテンツを復号し、コンテンツ 6B としての映像・音声情報またはデジタルデータを取り出す。

【0075】

(コンテンツ受信及び送信機 30 の受信機)

コンテンツ受信及び送信機 30 内の受信機も、図 9 に示したコンテンツ受信機と同様の構成を有し、コンテンツ作成機 22 からのコンテンツ (映像、音声またはデータ) を、コンテンツ 6A' として受信する。 40

【0076】

(その他)

図 4 において、ネットワーク 25、ネットワーク 10 は、インターネット等の通信ネットワークでメタデータの伝送を行う。

【0077】

放送網 11 は、既存の放送網で映像再生機間でコンテンツの配信をおこなう。

【0078】

次に、図 4 の実施例において、メタデータ制御機 8 及びコンテンツ受信機 9 の利用者も 50

、メタデータ追加を行った場合の動作を、以下に説明する。

【0079】

図4において、コンテンツ自身はあらかじめ作成しておき、コンテンツ作成機22に格納する。図4のコンテンツ作成機22の詳細なブロック図が図8である。

【0080】

図8において、コンテンツ6A(図4)はコンテンツ記憶部54で記憶される。コンテンツ作成機22は、コンテンツを暗号化してコンテンツ受信機9(或いはコンテンツ送信及び受信機30)に送信するため暗号化鍵(コンテンツ鍵Kc)をコンテンツごとに生成し、コンテンツを識別するためにコンテンツ識別を割り当て、コンテンツ識別毎にコンテンツ鍵を管理する。

10

【0081】

コンテンツはコンテンツ記憶部54より読み出され、符号化部55でMPEG-2TS(Transport Stream)に符号化される。符号化されたコンテンツはコンテンツ鍵生成部59で生成したコンテンツ鍵を使用してスクランブル部56で暗号化され、暗号化コンテンツとして生成される。

【0082】

メタデータからコンテンツへのアクセス制御を実現するためには、コンテンツにアクセス制御パラメータを埋め込む必要がある。そこで、メタデータアクセス制御情報生成部60でアクセス制御パラメータとなるメタデータアクセス制御記述子7Aを生成する。メタデータアクセス制御記述子7Aは、メタデータ制作者自身の識別コードであるメタデータ制作者識別と、メタデータ制作者の属性(コンテンツプロバイダー兼メタデータ制作者、専門メタデータ制作者、利用者(ユーザ)など)を示すメタデータ制作者種別とから構成される。

20

【0083】

メタデータ制作者種別を記述するメタデータアクセス制御記述子1のデータ構造は、図10の上表のようになる。メタデータ制作者識別を記述するメタデータアクセス制御記述子2のメタデータ構造は、図10の下表のようになる。

【0084】

図8において、生成されたコンテンツ識別、コンテンツ鍵及びメタデータアクセス制御情報は、Kc伝送用ECM/EMM生成部61でARIB STD-B25「デジタル放送におけるアクセス制御方式」で規定されるセクション形式のKc伝送用ECMまたはKc伝送用EMMとしてワーク鍵またはマスター鍵62で暗号化される。マスター鍵62は受信機毎に付与される共通鍵暗号化方式の暗号鍵であり、ワーク鍵62は事業者毎などの単位で付与される共通鍵暗号化方式の暗号鍵である。

30

【0085】

一方、図4のメタデータ制作者1は、メタデータ作成機2でコンテンツ6Aに対するメタデータ3Aを作成する。図6は、メタデータ作成機1の詳細なブロック図である。

【0086】

図6において、メタデータ制作者1は、コンテンツ6Aに対するメタデータ3Aをメタデータ作成機2のメタデータ作成部41で作成する。作成されるメタデータは、図2のようにARIB STD-B38に定義されているものに従ったXML形式の文書となる。メタデータ制作者1は、図2のようなXML形式のメタデータを作成した後、図3のように、作成したメタデータに対するメタデータ制作者署名4A(XML-Signatureに従う)を付与する。

40

【0087】

図3において、このメタデータ制作者署名4Aには制作者のメタデータ制作者公開鍵証明書5Aを含めておく。署名後のメタデータは、署名されたXML形式のメタデータ3Aのようになる。署名対象が文書全体或いは制作者1の作成部13とすると、XML署名文書は、XML-Signature Syntax and Processingに従った形式で制作者の署名4Aとしてメタデータに埋め込まれる。また、署名者の公開鍵証明書は、署名者の公開鍵証明書5Aのような形で、証明書のXML-Signatureの規格に従い、制作者の署名4Aに埋め込まれる。

50

【0088】

図4において、第一次制作者1が作成した、メタデータ3Aおよびコンテンツ6Aはネットワーク25を利用してコンテンツプロバイダーである第二次制作者に転送される（ここではメタデータ制作者34と表現する）。

【0089】

第二次制作者34は、第一次制作者1からメタデータを3A'として受信すると、図5に示すように、メタデータ制作者34の作成部37をメタデータ3A'に追加する。

【0090】

図5において、追加した後にメタデータ制作者34が作成した部分のみに対する署名処理を施し、メタデータ制作者34の署名39としてメタデータに付与する。このメタデータ制作者34の署名39には、第二次制作者34の公開鍵証明書であるメタデータ制作者公開鍵証明書を含めておく。このように、メタデータ制作者34の署名39がメタデータに埋め込まれる。

【0091】

図4において、コンテンツ6A'（6Aと同じ）及びメタデータ制作者34が作成したメタデータ3A'は、ネットワーク10及び放送網11を利用して、メタデータ3A'は利用者の端末であるメタデータ制御機8へメタデータ3Bとして配信し、コンテンツ6A'はコンテンツ受信機9へコンテンツ6Bとして配信される。利用者は、配信されたメタデータ3Bに付加されているメタデータ制作者1の署名であるメタデータ制作者の署名4A、メタデータ制作者34の署名であるメタデータ制作者の署名39（図5）を検証し、メタデータ3Bが改竄されていないことを確認する。その後、利用者は、メタデータ3Bに、図5における作成部37と同様に、自分でメタデータ追加を利用者の作成部に作成し、図5における署名39と同様に、自分の署名を追加することができる。

【0092】

この場合、利用者は、自分でメタデータ追加を施したメタデータ3Bを用いたコンテンツ6Bのダイジェスト版の再生を実行する。このとき、メタデータ3Bには、再生対象のコンテンツ6BのフラグメントがARIB STD-B38に従った<SegmentInformation...> ... </SegmentInformation>というタグの中に記述されており、その情報に従ってコンテンツ6Bのダイジェストの再生をコンテンツ受信機9に命令する。再生時には、本発明の最も重要な特徴であるメタデータ3Bからコンテンツ6Bへのアクセス制御情報をチェックしてから再生する。メタデータ3Bからコンテンツ6Bへのアクセス可・不可は、次のような手順で判断される。

【0093】

手順1. メタデータ3Bに含まれる第1の署名（メタデータ制作者1の署名4A）、第2の署名（メタデータ制作者34の署名39）、及び第3の署名（メタデータ制御機8及びコンテンツ受信機9の利用者の署名）を検証し、同時に署名の検証に必要な証明書も検証する。

【0094】

手順2. メタデータ内の利用対象の部位を作成したのは誰かをその部分に対して付加されている署名から識別する。このとき、第1乃至第3の署名（XML署名形式の署名文書）の中にそれぞれ含まれているメタデータ制作者の公開鍵証明書の所有者から、所有者名および所有者の所属組織を特定する。公開鍵証明書の所有者属性はDN（Distinguished Name）とよばれる形式で表現され、cnの値は所有者名が登録され、ouの値を所有者所属組織が登録されている。また、cnの値は、図10のメタデータアクセス制御識別と同じ命名規則が適用され、ouの値は、図10のメタデータアクセス制御種別と同じ命名規則が適用される。

【0095】

手順3. 一方、コンテンツ受信機（再生機）9には、コンテンツ作成時にコンテンツ作成機22のメタデータアクセス制御情報生成部60（図8）で作成された、図10の2つの表に従ったアクセス制御情報が、メタデータアクセス制御識別子7Aとしてコンテンツ

6 Aと一緒に配信される。そこで、コンテンツ受信機（再生機）9にメタデータ制御機8から問い合わせるメタデータアクセス制御識別子7 Aの情報を取得する。

【0096】

手順4. この際、図9のコンテンツ受信機（再生機）9は、メタデータ制御機8からの要求により、メタデータアクセス制御情報記憶部7 3からメタデータアクセス制御情報7 5（メタデータアクセス制御識別子7 A）を取り出し返却する。

【0097】

手順5. コンテンツ受信機（再生機）9から返却されたメタデータアクセス制御記述子7 Aのメタデータアクセス制御識別及びメタデータアクセス制御種別と、利用対象となるメタデータを作成した3人の作成者の証明書の所有者属性のcn及びouとを付き合わせ、3人の作成者の証明書の所有者属性のcn及びouがメタデータアクセス制御記述子7 Aのメタデータアクセス制御識別及びメタデータアクセス制御種別と一致するか否かを判定することにより、アクセス制御を実現する。

【0098】

3人の作成者の証明書の所有者の少なくとも一つが、メタデータアクセス制御記述子7 A中に記述されていれば、メタデータ3 Bのうちのその所有者の作成した情報からはコンテンツ6 Bへのアクセスが許可される。アクセスが許可された場合は、許可されたメタデータ3 Bの情報に従ってコンテンツ受信機（再生機）9へコンテンツ6 Bの部分再生やその他の情報の表示を命令する。コンテンツ受信機（再生機）9は指示に従いコンテンツ6 Bを部分再生する。

【0099】

以上説明したように、本発明の実施例は、別々に配信されるARIB STD-B38で定められた形式のメタデータ及びコンテンツにおいて、メタデータからコンテンツに対するアクセスの可否を、メタデータの署名者の公開鍵証明書の所有者の情報とコンテンツに埋め込まれたメタデータアクセス制御記述子を付き合わせるにより制御することを特徴とする。

【0100】

本発明の実施例によれば、メタデータの作成者の署名値中の公開鍵証明書の所有者の情報とコンテンツに埋め込まれたメタデータアクセス制御記述子を付き合わせるにより、メタデータからコンテンツへのアクセス可否を判断することが出来る。

【0101】

更に、本発明の実施例によれば、証明書の所有者の情報に適切な階層構造をもたせ、その階層構造に対応したメタデータアクセス制御記述子（図10のメタデータアクセス制御記述子1及び2）を定義することで、メタデータの作成者の組織属性に従ったメタデータからコンテンツへのアクセス制御を実現することが出来る。

【0102】

なお、上述した実施例の説明では、図8に示したように、コンテンツと、識別子（メタデータアクセス制御記述子）を含んだライセンス情報（Kc伝送用ECM/EMM）とを多重化手段6 3で多重化して、送信したが、コンテンツとライセンス情報は、かならずしも併せて送る必要はなく、たとえば、コンテンツのみを送信しておき、後で、識別子（メタデータアクセス制御記述子）を埋め込んだライセンス情報（Kc伝送用ECM/EMM）を送信するといった手段を取ることも可能である。

【図面の簡単な説明】

【0103】

【図1】本発明の第1の実施例によるアクセス制御システムのブロック図である。

【図2】図1のアクセス制御システムのメタデータ作成機において、メタデータ制作者1によって作成された署名前メタデータを示す図である。

【図3】図1のアクセス制御システムのメタデータ作成機において、作成者付きのメタデータを示す図である。

【図4】本発明の第2の実施例によるアクセス制御システムのブロック図である。

【図5】図4のアクセス制御システムのメタデータ制御機において、追加編集を加えた、

10

20

30

40

50

署名されたメタデータを示す図である。

【図 6】図 4 のアクセス制御システムのメタデータ作成機のブロック図である。

【図 7】図 4 のアクセス制御システムのメタデータ制御機のブロック図である。

【図 8】図 4 のアクセス制御システムのコンテンツ作成機内の送信機のブロック図である。

。

【図 9】図 4 のアクセス制御システムのコンテンツ受信機のブロック図である。

【図 10】図 4 のアクセス制御システムで用いられるメタデータアクセス制御記述子を説明するための図である。

【符号の説明】

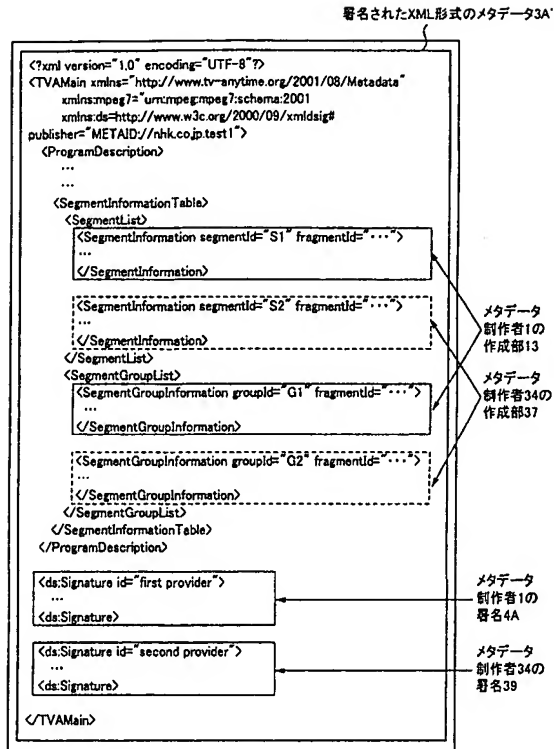
【0104】

10

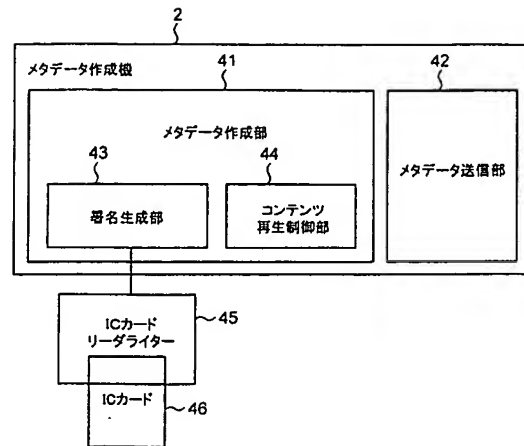
- 1 メタデータ制作者
- 2 メタデータ作成機
- 3 A メタデータ
- 3 A' メタデータ
- 4 A XML署名
- 5 A 公開鍵証明書
- 6 A コンテンツ
- 6 A' コンテンツ
- 7 A メタデータアクセス制御記述子
- 8 メタデータ制御機
- 9 コンテンツ受信機
- 10 ネットワーク
- 11 放送網
- 13 制作者の作成部
- 22 コンテンツ作成機
- 25 ネットワーク
- 29 メタデータ制御機
- 30 コンテンツ受信及び送信機
- 34 メタデータ制作者

20

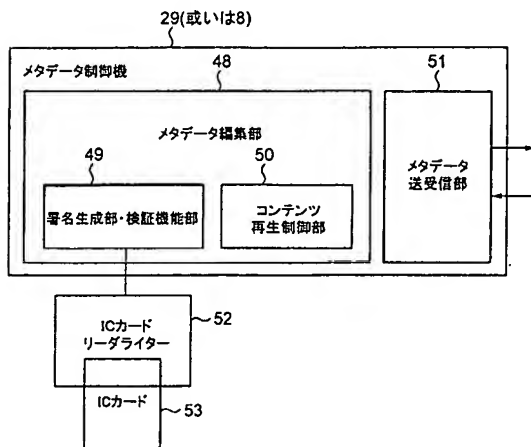
【図 5】



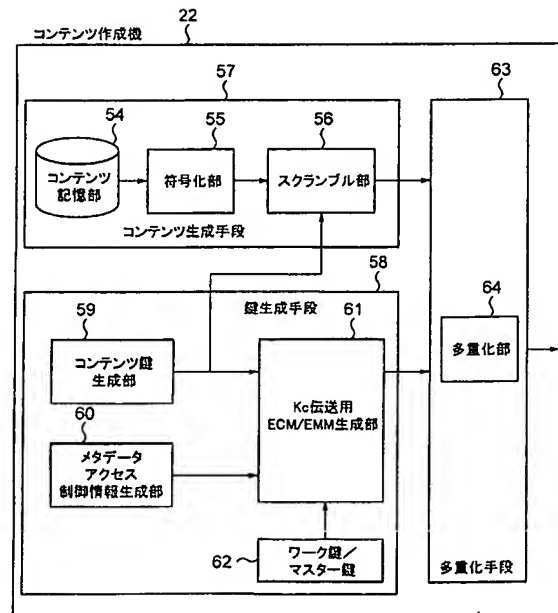
【図 6】



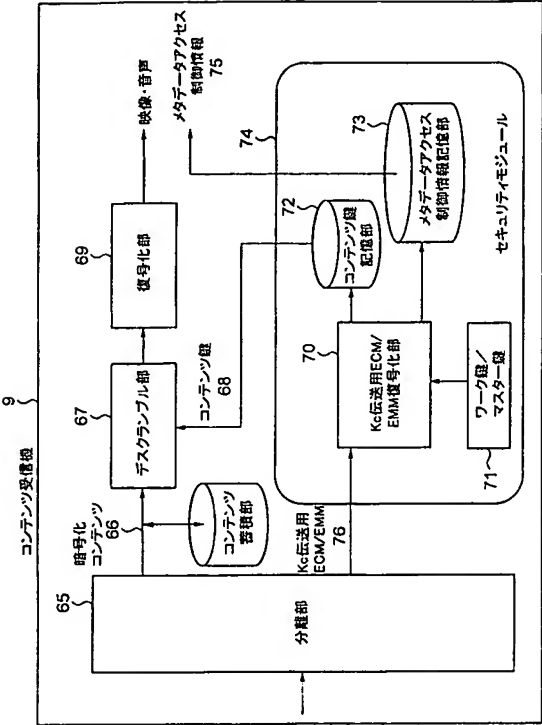
【図 7】



【図 8】



【図 9】



【図 10】

記述子名	項目名	バイト長	備考
メタデータ アクセス制御記述子 1	記述子タグ	1	
	記述子長	1	メタデータ制作者識別をN箇列装した場合、 値はN×10となる
	メタデータ制作者識別	10	最大10箇まで列挙する
メタデータ アクセス制御記述子 2	記述子タグ	1	
	記述子長	1	メタデータ制作者識別をN箇列装した場合、 値はN×10となる
	メタデータ制作者識別	10	最大10箇まで列挙する

フロントページの続き

(72)発明者 馬場 秋継

東京都世田谷区砧一丁目10番11号 日本放送協会放送技術研究所内

(72)発明者 中村 晴幸

東京都世田谷区砧一丁目10番11号 日本放送協会放送技術研究所内

(72)発明者 石川 清彦

東京都世田谷区砧一丁目10番11号 日本放送協会放送技術研究所内

(72)発明者 栗岡 辰弥

東京都渋谷区神南二丁目2番1号 日本放送協会放送センター内

Fターム(参考) 5B017 AA07 BA06 BA07 CA15

5J104 AA07 AA09 KA01 KA04 LA03 LA06 NA02 NA27 NA38 PA14